

1 Claim 11

2 A user authentication system comprising:

3 the user authentication apparatus for said prover  
4 computer according to claim 9; and

5 a plurality of user authentication apparatuses for  
6 said verifier computers according to claim 10.

7 Claim 12

8 A user authentication system, wherein a one-way function  
9  $F$ , which should satisfy  $v = F(g, -s)$ , is determined by  
10 employing an integer  $g$ , which is defined in advance, for  
11 the relation between a public key  $v$  and a secret key  $s$   
12 of a prover computer, and wherein a relation is verified  
13 between said prover computer and each of multiple  
14 verifier computers, comprising:

15 transmission means, for said prover computer, for  
16 generating a random number  $a$  and obtaining a cryptogram  
17  $A = \text{the function } F(g, a)$ , and for transmitting said  
18 obtained cryptogram  $A$  to said verifier computers;

19 reception means for said verifier computers, for  
20 receiving said cryptogram  $A$  from said prover computer;

21 transmission means for said verifier computers, for  
22 generating a random number  $b$  with which said cryptogram  
23  $A$  is employed to obtain a cryptogram  $B = \text{the function}$   
24  $F(g, b)$  and a cryptogram  $X = \text{the function } F(A, b)$ , and  
25 for transmitting said cryptograms  $B$  and  $X$  to said prover  
26 computer;

27 reception means for said prover computer, for  
28 receiving said cryptograms  $B$  and  $X$  from said verifier

1 computers;

2 verification means for said prover computer, for  
3 employing said cryptograms B and X to determine whether  
4 a relation of said cryptogram  $X = \text{the function } F(B, a)$   
5 has been established;

6 cryptogram computation means for said prover  
7 computer, for generating a random number c when it is  
8 ascertained that said relation has been established, and  
9 for obtaining said cryptogram  $C = \text{the function } F(g, c)$   
10 and said cryptogram  $Y = \text{the function } F(B, c)$ , or said  
11 cryptogram  $C = \text{the function } F(A, c)$  and said cryptogram  
12  $Y = \text{the function } F(X, c)$ , and a cryptogram  $Z = \text{the}$   
13 function  $H(a, Y, s)$ ; and

14 cryptogram transmission means for said prover  
15 computer, for transmitting said cryptograms C, Y and Z  
16 to said verifier computers;

17 cryptogram reception means, for said verifier  
18 computers, for receiving said cryptograms C, Y and Z  
19 from said prover computer; and

20 verification means for said verifier computers, for  
21 employing said cryptograms C, Y and Z that are received  
22 to verify a relation between said verifier computers and  
23 said prover computer when two relations of said  
24 cryptogram  $Y = \text{the function } F(C, b)$  and said cryptogram  
25  $A = \text{the function } J(v, Y, g, Z)$  are established at the  
26 same time.

27 13. A computer program product comprising a computer  
28 usable medium having computer readable program code means  
29 embodied therein for causing user authentication, the

1 computer readable program code means in said computer  
2 program product comprising computer readable program code  
3 means for causing a computer to effect the apparatus of  
4 claim 9.

5 14. A computer program product comprising a computer  
6 usable medium having computer readable program code means  
7 embodied therein for causing user authentication, the  
8 computer readable program code means in said computer  
9 program product comprising computer readable program code  
10 means for causing a computer to effect the apparatus of  
11 claim 10.

12 15. A computer program product comprising a computer  
13 usable medium having computer readable program code means  
14 embodied therein for causing user authentication, the  
15 computer readable program code means in said computer  
16 program product comprising computer readable program code  
17 means for causing a computer to effect the system of  
18 claim 11.

19 16. A computer program product comprising a computer  
20 usable medium having computer readable program code means  
21 embodied therein for causing user authentication, the  
22 computer readable program code means in said computer  
23 program product comprising computer readable program code  
24 means for causing a computer to effect the system of  
25 claim 12.

26 17. An article of manufacture comprising a computer

1 usable medium having computer readable program code means  
2 embodied therein for implementing a user authentication  
3 method, the computer readable program code means in said  
4 article of manufacture comprising computer readable  
5 program code means for causing a computer to effect the  
6 steps of claim 1.

11/01/2000 10:00 AM